数理解析研究所講究録
第 1665 巻 2009 年 60-66

TALK SUMMARY

1. The Riemann Zeta-Function and Hecke Congruence Subgroups.
2. Three problems of Atle Selberg (1917–2007)

Delivered on 18 October 2007
Workshop on Analytic Number Theory
RIMS Kyoto University

BY YOICHI MOTOHASHI

0. IN THE FIRST TALK we presented a succinct account of our recent work [10]. That is in fact a rework of our old file on an explicit spectral decomposition of the mean value

$$M_2(g;A)=\int_{-\infty}^{\infty}\left|\zeta(\tfrac{1}{2}+it)\right|^4\left|A(\tfrac{1}{2}+it)\right|^2 g(t)dt, \tag{0.1}$$

which has been left unpublished since September 1994, though its summary account is given in [6] (see also [8, Section 4.6]). Here

$$A(s)=\sum_n \alpha_n n^{-s} \tag{0.2}$$

is a finite Dirichlet series and g an appropriate test function. At this occasion we included (1) a rigorous treatment of generalized Kloosterman sums associated with arbitrary $\Gamma_0(q)$, (2) an in-depth treatment of the Mellin transform

$$Z_2(s;A)=\int_{1}^{\infty}\left|\zeta(\tfrac{1}{2}+it)\right|^4\left|A(\tfrac{1}{2}+it)\right|^2 t^{-s}dt. \tag{0.3}$$

Because of their independent interest, we shall give the most salient aspects of these two subjects in the following sections.

IN THE SECOND TALK we discussed the three problems which had been personally shown to us by Atle Selberg who passed away on 6 August 2007. With this, we tried to briefly relate three of his many great contributions to mathematics – the elementary proof of the prime number theorem, the Λ^2-sieve, and the theory of the zeta-functions. Details of this part of our talk will be published in a future occasion.

1. Let Γ be a discrete subgroup of $\mathrm{PSL}(2,\mathbb{R})$ which has a fundamental domain of finite volume. We call $\mathfrak{a}\in\mathbb{R}\cup\infty$ a cusp of Γ if and only if there exists a $\sigma\in\Gamma$ such that σ is parabolic and $\sigma(\mathfrak{a})=\mathfrak{a}$. Let $\Gamma_{\mathfrak{a}}$ be the stabilizer of $\mathfrak{a}$. There exits a $\sigma_{\mathfrak{a}}$ such that $\sigma_{\mathfrak{a}}(\infty)=\mathfrak{a}$

and $\sigma_{\mathfrak{a}}^{-1}\Gamma_{\mathfrak{a}}\sigma_{\mathfrak{a}} = \Gamma_\infty = [S]$ with $S = \left(\begin{smallmatrix}1 & 1\\ & 1\end{smallmatrix}\right)$. Then a generalized Kloosterman sum associated with the two cusps $\mathfrak{a}, \mathfrak{b}$ of Γ is defined to be the trigonometrical sum

$$S(m, n; c; \mathfrak{a}, \mathfrak{b}) = \sum_{\mathrm{g}} \exp\left(2\pi i(am + dn)/c\right), \tag{1.1}$$

where g runs over the representatives of $\Gamma_{\mathfrak{a}}\backslash\Gamma/\Gamma_{\mathfrak{b}}$ such that $\sigma_{\mathfrak{a}}^{-1}\mathrm{g}\sigma_{\mathfrak{b}} = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ with the same $c > 0$. This does not depend on the choice of $\sigma_{\mathfrak{a}}$, $\sigma_{\mathfrak{b}}$, modulo a unitary multiplier.

In order to develop the sum formulas of R.W. Bruggeman and N.V. Kuznetsov over Γ, or the spectral theory of sums of $S(m, n; c; \mathfrak{a}, \mathfrak{b})$, we need first of all to prove that there exists a constant $\tau < 2$ such that for any non-zero integers m, n and for any pair of cusps $\mathfrak{a}, \mathfrak{b}$

$$\sum_c \frac{1}{c^\tau} |S(m, n; c; \mathfrak{a}, \mathfrak{b})| \ll |mn|^\eta, \tag{1.2}$$

with an appropriate constant η, where c runs over all positive values with which (1.1) is defined. In the case of the full modular group, this is a consequence of non-trivial bounds, such as Weil's, for ordinary Kloosterman sums. In literature it is often claimed either explicitly or implicitly that the same holds with any Hecke congruence subgroup $\Gamma_0(q)$. However, it appears to us that until recently no rigorous proof of this fundamental assertion had been given in print, excepting [6] and [7] where the case with q square-free is explicitly discussed. With this situation, Bruggeman provided us with a treatment [1] of the sums using a partly adelic reasoning; and it is now assured that (1.2) indeed holds with any $\Gamma_0(q)$. Here we shall prove the same with an alternative elementary method.

Thus, we note that a complete representative set of cusps inequivalent mod $\Gamma_0(q)$ is given by

$$\left\{\frac{u}{w} : w|q,\ (u, w) = 1,\ u \bmod (w, q/w)\right\}. \tag{1.3}$$

We have

$$\Gamma_{u/w} = \left\{\begin{pmatrix} 1 + \nu\dfrac{u}{w} & -\nu\dfrac{u^2}{w^2} \\ \nu & 1 - \nu\dfrac{u}{w}\end{pmatrix} : \nu \equiv 0 \bmod [w^2, q]\right\}. \tag{1.4}$$

We write

$$q = cd = vw = (v, w)^2 v^* w^*, \quad v^* = \frac{v}{(v, w)},\ w^* = \frac{w}{(v, w)}; \tag{1.5}$$

then we may put

$$\sigma_{u/w} = \varpi_{u/w}\tau_{v^*}, \tag{1.6}$$

where

$$\varpi_{u/w} = \begin{pmatrix} u & \dfrac{u\overline{u} - 1}{w} \\ w & \overline{u}\end{pmatrix}, \quad \tau_{v^*} = \begin{pmatrix}\sqrt{v^*} & \\ & \dfrac{1}{\sqrt{v^*}}\end{pmatrix}, \tag{1.7}$$

with $u\overline{u} \equiv 1 \bmod w$. In fact we have

$$\Gamma_{u/w} = \sigma_{u/w}\Gamma_\infty\sigma_{u/w}^{-1} = \varpi_{u/w}\left[S^{v^*}\right]\varpi_{u/w}^{-1}. \tag{1.8}$$

With this, we rewrite the Kloosterman sum $S(m,n;c;u_1/w_1,u_2/w_2)$ with u_i/w_i in (1.3) and (1.6) in force, employing the Bruhat decomposition; that is, in the big cell of $\mathrm{PSL}(2,\mathbb{R})$ we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & a/c \\ & 1 \end{pmatrix}\begin{pmatrix} & -1/c \\ c & \end{pmatrix}\begin{pmatrix} 1 & d/c \\ & 1 \end{pmatrix} = B[a,d;c], \tag{1.9}$$

say. Let $\varkappa_q$ be the characteristic function of the set $\Gamma_0(q) \subset \mathrm{PSL}(2,\mathbb{R})$. Then we have

$$\begin{aligned} &S(m,n;c;u_1/w_1,u_2/w_2) \\ &= \sum_{\substack{ad\equiv 1 \bmod c \\ a \bmod v_1^* c \\ d \bmod v_2^* c}} \varkappa_q\left(\varpi_{u_1/w_1}B[a,d;c]\varpi_{u_2/w_2}^{-1}\right)\exp\left(2\pi i\left(\frac{ma}{v_1^*c}+\frac{nd}{v_2^*c}\right)\right), \end{aligned} \tag{1.10}$$

where v_i^* and ϖ_{u_i/w_i} are as in (1.5) and (1.7). In fact, it suffices to observe that the Kloosterman sum on the left is associated with the double coset decomposition

$$\begin{aligned} \Gamma_{u_1/w_1}\backslash\Gamma_0(q)/\Gamma_{u_2/w_2} &= \varpi_{u_1/w_1}\left[S^{v_1^*}\right]\backslash\varpi_{u_1/w_1}^{-1}\Gamma_0(q)\varpi_{u_2/w_2}/\left[S^{v_2^*}\right]\varpi_{u_2/w_2}^{-1} \\ &= \varpi_{u_1/w_1}\Gamma_\infty\backslash\tau_{v_1^*}^{-1}\varpi_{u_1/w_1}^{-1}\Gamma_0(q)\varpi_{u_2/w_2}\tau_{v_2^*}/\Gamma_\infty\varpi_{u_2/w_2}^{-1}, \end{aligned} \tag{1.11}$$

as (1.8) holds. We remark also that $\varkappa_q\left(\varpi_{u_1/w_1}B[a,d;c]\varpi_{u_2/w_2}^{-1}\right)$ is a function of $a \bmod v_1^*c$, $d \bmod v_2^*c$. To see this, we note the relation

$$\begin{aligned} &\varpi_{u_1/w_1}B[a+a',d+d';c]\varpi_{u_2/w_2}^{-1} \\ =&\varpi_{u_1/w_1}\begin{pmatrix} 1 & a'/c \\ & 1 \end{pmatrix}\varpi_{u_1/w_1}^{-1}\cdot\varpi_{u_1/w_1}B[a,d;c]\varpi_{u_2/w_2}^{-1}\cdot\varpi_{u_2/w_2}\begin{pmatrix} 1 & d'/c \\ & 1 \end{pmatrix}\varpi_{u_2/w_2}^{-1}; \end{aligned} \tag{1.12}$$

and

$$\begin{aligned} \varpi_{u_1/w_1}\begin{pmatrix} 1 & a'/c \\ & 1 \end{pmatrix}\varpi_{u_1/w_1}^{-1} \in \Gamma_{u_1/w_1} \subset \Gamma_0(q), \\ \varpi_{u_2/w_2}\begin{pmatrix} 1 & d'/c \\ & 1 \end{pmatrix}\varpi_{u_2/w_2}^{-1} \in \Gamma_{u_2/w_2} \subset \Gamma_0(q), \end{aligned} \tag{1.13}$$

provided $v_1^*|(a'/c)$, $v_2^*|(d'/c)$, which proves the assertion.

Next, we shall show that if $ad \equiv 1 \bmod c$, then

$$\varkappa_q\left(\varpi_{u_1/w_1}B[a,d;c]\varpi_{u_2/w_2}^{-1}\right) = \varkappa_q\left(\varpi_{\overline{c^*}u_1/w_1}B[a,d;c_0]\varpi_{\overline{c^*}u_2/w_2}^{-1}\right), \tag{1.14}$$

where $c = c_0c^*$ with $c_0 = (c, q^\infty)$, and $\overline{c^*}c^* \equiv 1 \bmod q$; note that $\overline{c^*}u_i/w_i$ are cusps of $\Gamma_0(q)$. In fact, computing the lower-left element of $\varpi_{u_1/w_1}B[a,d;c]\varpi_{u_2/w_2}^{-1}$, we see that the value of the left side equals 1 if and only if

$$\overline{u_2}(aw_1 + c\overline{u}_1) \equiv w_2\,(w_1(ad-1)/c + d\overline{u_1}) \bmod q; \tag{1.15}$$

and this is equivalent to the congruence

$$\overline{\overline{c^*}u_2}(aw_1 + c_0\overline{\overline{c^*}u_1}\,) \equiv w_2\left(w_1(ad-1)/c_0 + d\overline{\overline{c^*}u_1}\right) \bmod q, \tag{1.16}$$

which immediately implies (1.14).

Hence we have

$$\begin{aligned} &S(m,n;c;u_1/w_1,u_2/w_2)\\ &= \sum_{\substack{ad\equiv 1 \bmod c\\ a \bmod v_1^*c\\ d \bmod v_2^*c}} \varkappa_q\left(\varpi_{\overline{c^*}u_1/w_1}B[a,d;c_0]\varpi_{\overline{c^*}u_2/w_2}^{-1}\right)\exp\left(2\pi i\left(\frac{ma}{v_1^*c}+\frac{nd}{v_2^*c}\right)\right). \end{aligned} \tag{1.17}$$

Here we have

$$\frac{1}{v_i^*c} \equiv \frac{\widetilde{c_i^*}}{v_i^*c_0} + \frac{\widetilde{v_i^*c_0}}{c^*} \bmod 1, \tag{1.18}$$

with $\widetilde{c_i^*}c^* \equiv 1 \bmod v_ic_0$, $\widetilde{v_i^*c_0}v_i^*c_0 \equiv 1 \bmod c^*$. Inserting this into (1.17), putting $a \equiv a_0 \bmod v_1^*c_0$, $a \equiv a^* \bmod c^*$, $d \equiv d_0 \bmod v_1^*c_0$, $d \equiv d^* \bmod c^*$, and further, noting the congruence property of $\varkappa_q$ shown above, we may rewrite (1.17) as

$$\begin{aligned} S(m,n;c;u_1/w_1,u_2/w_2) = &\sum_{\substack{ad\equiv 1 \bmod c\\ a \bmod v_1^*c\\ d \bmod v_2^*c}} \varkappa_q\left(\varpi_{\overline{c^*}u_1/w_1}B[a_0,d_0;c_0]\varpi_{\overline{c^*}u_2/w_2}^{-1}\right)\\ &\times \exp\left(2\pi i\left(\frac{\widetilde{c_1^*}ma_0}{v_1^*c_0}+\frac{\widetilde{c_2^*}nd_0}{v_2^*c_0}\right)\right)\cdot\exp\left(2\pi i\left(\frac{\widetilde{v_1^*c_0}ma^*}{c^*}+\frac{\widetilde{v_2^*c_0}n\delta^*}{c^*}\right)\right). \end{aligned} \tag{1.19}$$

We have thus obtained the factorization

$$\begin{aligned} &S(m,n;c;u_1/w_1,u_2/w_2)\\ &\quad = S(\widetilde{c_1^*}m,\widetilde{c_2^*}n;c_0;\overline{c^*}u_1/w_1,\overline{c^*}u_2/w_2)S(\widetilde{v_1^*c_0}m,\widetilde{v_2^*c_0}n;c^*), \end{aligned} \tag{1.20}$$

where the last factor is an ordinary Kloosterman sum. In particular, the Weil bound yields that

$$S(m,n;c;u_1/w_1,u_2/w_2) \ll qc_0((m,n,c^*)c^*)^{\frac{1}{2}+\varepsilon}, \tag{1.21}$$

with the implied constant depending only on ε an arbitrary small positive constant. Therefore, we have obtained

Theorem 1. *Any $\Gamma_0(q)$ satisfies (1.2) with $\tau > \frac{3}{2}$.*

REMARK. The decomposition (1.20) extends to a full localization, with which we may replace (1.21) by the best possible bound. To this we shall return elsewhere.

2. Our argument reduces $M_2(g;A)$ to sums of Kloosterman sums $S(m, \bar{d}n; ck)$ where $(ck, d) = 1$ and $d\bar{d} \equiv 1 \bmod ck$. To capture these sums, we consider the combination of the cusps $1/q$ and $1/c$ of the group $\Gamma_0(q)$, $q = cd$.

However, we first modify (1.6) as

$$\sigma_{u/w} = \xi_{u/w}\tau_{v^*}, \quad \xi_{u/w} = \varpi_{u/w}S^{f/(v,w)}, \tag{2.1}$$

with

$$fw^* \equiv -\bar{u} \bmod v^*, \quad u\bar{u} \equiv 1 \bmod w. \tag{2.2}$$

A simple congruence consideration gives that for any $v_i w_i = q$ with $(v_i, w_i) = 1$,

$$\xi_{1/w_1}^{-1}\Gamma_0(q)\xi_{1/w_2} = \left\{ \begin{pmatrix} (v_1,w_2)k & (v_1,v_2)l \\ (w_1,w_2)r & (w_1,v_2)s \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}),\ k,l,r,s \in \mathbb{Z} \right\} \tag{2.3}$$

(cf. [4, p. 534]; note that there q is square-free but here not assumed to be so). We then have

$$\Gamma_{1/w_1}\backslash\Gamma_0(q)/\Gamma_{1/w_2} = \sigma_{1/w_1}\Gamma_\infty\tau_{v_1}^{-1}\xi_{1/w_1}^{-1}\backslash\Gamma_0(q)/\xi_{1/w_2}\tau_{v_2}\Gamma_\infty\sigma_{1/w_2}^{-1}$$

$$\Longleftrightarrow \quad \Gamma_\infty\backslash\tau_{v_1}^{-1}\xi_{1/w_1}^{-1}\Gamma_0(q)\xi_{1/w_2}\tau_{v_2}/\Gamma_\infty$$

$$\Longleftrightarrow \quad \Gamma_\infty\backslash\left\{ \begin{pmatrix} (v_1,w_2)r\sqrt{v_2/v_1} & (v_1,v_2)l/\sqrt{v_1v_2} \\ (w_1,w_2)k\sqrt{v_1v_2} & (w_1,v_2)s\sqrt{v_1/v_2} \end{pmatrix} \right\}/\Gamma_\infty$$

$\Longleftrightarrow$ classifying the solutions of $(v_1,w_2)(w_1,v_2)rs - (w_1,w_2)(v_1,v_2)kl = 1$
according to $(v_1,w_2)r\sqrt{v_2/v_1}, (w_1,v_2)s\sqrt{v_1/v_2} \bmod (w_1,w_2)k\sqrt{v_1v_2}$

$\Longleftrightarrow$ the moduli of the generalized Kloosterman sums have the form $(w_1,w_2)k\sqrt{v_1v_2}$
with $((v_1,w_2)(w_1,v_2),k) = 1$ and
$(v_1,w_2)(w_1,v_2)rs \equiv 1 \bmod (w_1,w_2)(v_1,v_2)k$
$(v_1,w_2)r \bmod v_1(w_1,w_2)r \longleftrightarrow r \bmod (v_1,v_2)(w_1,w_2)k$

$$(w_1, v_2)s \bmod v_2(w_1, w_2)k \longleftrightarrow s \bmod (v_1, v_2)(w_1, w_2)k$$

$$\begin{aligned}
\Longleftrightarrow \quad & \gamma = (w_1, w_2)k\sqrt{v_1 v_2}, \ ((v_1, w_2)(w_1, v_2), k) = 1, \\
& S(m, n; \gamma; 1/w_1, 1/w_2) = \sum_{\substack{r,s \bmod (v_1,v_2)(w_1,w_2)k \\ (v_1,w_2)(w_1,v_2)rs \equiv 1 \bmod (v_1,v_2)(w_1,w_2)k}} \exp\left(\frac{2\pi i(rm+ns)}{(v_1,v_2)(w_1,w_2)k}\right) \\
& \qquad = S(\overline{(v_1, w_2)}m, \overline{(w_1, v_2)}n; (v_1, v_2)(w_1, w_2)k),
\end{aligned} \tag{2.4}$$

where the last member is an ordinary Kloosterman sum. In particular, we find that if $q = cd$, $(c, d) = 1$, and $(k, d) = 1$, then

$$S(m, n; ck\sqrt{d}; 1/q, 1/c) = S(m, \overline{d}n; ck) \tag{2.5}$$

under the specification (2.1).

A combination of Theorem 1 and (2.5) allows us to decompose $M_2(g; A)$ according to the spectral structure of the space of cusp forms over $\Gamma_0(q)$ with varying q; the details are fully developed in [10] which is quite involved as might be expected.

It then transpires that

Theorem 2. *Provided $\alpha_n > 0$ for square-free n and $= 0$ otherwise, the function $Z_2(s; A)$ has infinitely many simple poles on the line $\mathrm{Re}\, s = \frac{1}{2}$, which come from eigenvalues of the hyperbolic Laplacian acting over the space of $\Gamma_0(q)$-automorphic forms with q varying.*

This restriction on α_n is made solely for the sake of a convenience to develop the relevant discussion in [10]. It can be lifted in various fashions.

Our result suggests strongly that the Mellin transform

$$Z_3(s; 1) = \int_1^\infty \left|\zeta\left(\tfrac{1}{2} + it\right)\right|^6 t^{-s} dt \tag{2.6}$$

should have the line $\mathrm{Re}\, s = \frac{1}{2}$ as a natural boundary, for $|\zeta|^6 = |\zeta|^4|\zeta|^2$ and $|\zeta|^2$ may be replaced by a finite expression similar to $|A|^2$ via the approximate functional equation. The same has been speculated also by a few people other than us (see [3][5] for instance), but it appears that our theorem is so far the sole explicit evidence supporting this conjectural assertion. It entails naturally

Problem: Is the set $\bigcup_{q \ge 1} \mathrm{Sp}(\Gamma_0(q))$ dense in the half line $\left(\frac{1}{4}, \infty\right)$?

3. Here are additional discussion: As we noted already at a few occasions, the reason of the success with $M_2(g; 1)$ lies definitely in the fact that the Eisenstein series in the framework of $\mathrm{SL}(2, \mathbb{R})$ is closely related to the product of two zeta-values and in that the group is of real rank one, with the observation that the later is reflected in that the integral for $M_2(g; 1)$ is single (as is inferred from the arguments developed in e.g. [2][9]). Extrapolating this, we surmise that a proper formulation of the sixth moment of the zeta-function be expressed in terms of a double integral unlike $M_2(g;1)$, and thus $Z_3(s;1)$ be replace by a double Mellin transform, for the group $\mathrm{SL}(3,\mathbb{R})$ is closely related to the product of three zeta-values and it is of real rank 2. Nevertheless, it seems worth considering $M_2(g;A)$, as it stands between the pure fourth and sixth moments and requires less machineries than the plausible direct approach to the sixth moment via the spectral theory of $L^2(\mathrm{PSL}(3,\mathbb{Z})\backslash\mathrm{PSL}(3,\mathbb{R}))$ such as proposed in [8, Section 5.4].

We comment further that in order to deal with $M_2(g;A)$ there are at least three ways for us to proceed along. The first is the argument that we took in [8], the second is a representation theoretic approach developed in [2], and the third is the one in [9] which is more representation theoretic and in fact generalizes to quite a wide extent. We took in [10] again the first way, for it appears to be the most explicit and allow us to exploit best the peculiarity of our problem, i.e., the presence of the square of the zeta-function in place of the first power of an automorphic L-function. Nevertheless, it should be stressed that the methods in [2] and [9] have a definite advantage over that in [8], for they are independent of the spectral theory of Kloosterman sums.

References

[1] R. Bruggeman. Kloosterman sums (v.5). September 2007.

[2] R. Bruggeman and Y. Motohashi. A new approach to the spectral theory of the fourth moment of the Riemann zeta-function. J. reine angew. Math., **579** (2005), 75–114.

[3] A. Diaconu. The function $\mathcal{Z}_3(w)$ has natural boundary. Notes of October 24, 2006.

[4] D.A. Hejhal. *The Selberg Trace Formula for* $\mathrm{PSL}(2,\mathbb{R})$. II. Lect. Notes in Math., vol. **1001**, Springer-Verlag, Berlin, 1983.

[5] A. Ivić. Remarks on the natural boundary of $\mathcal{Z}_k(s)$. Notes of October 25, 2006.

[6] Y. Motohashi. The Riemann zeta-function and Hecke congruence subgroups. RIMS Kyoto Univ. Kokyuroku, **958** (1996), 166–177.

[7] —. The mean square of Dedekind zeta-functions of quadratic number fields. In: *Sieve Methods, Exponential Sums and their Applications in Number Theory* (G.R.H. Greaves, G. Harman, M.N. Huxley, editors) Cambridge University Press, Cambridge 1997, pp. 309–323.

[8] —. *Spectral Theory of the Riemann Zeta-Function*. Cambridge University Press, Cambridge 1997.

[9] —. A note on the mean value of the zeta and L-functions. XV. Proc. Japan Acad., **83A** (2007), 73–78.

[10] —. The Riemann zeta-function and Hecke congruence subgroups. II. arXiv:0709.2590v2 [math.NT].

Department of Mathematics, Nihon University
Surugadai, Tokyo 101-8308, JAPAN
www.math.cst.nihon-u.ac.jp/~ymoto/